Department of Justice Canada | Ministère de la Justice Canada

Canada



**NOTES FOR A SPEECH BY**
**THE HONORABLE ANNE MCLELLAN**
**MINISTER OF JUSTICE**
**ATTORNEY GENERAL OF CANADA**

# TO

# 10TH CONGRESS ON PREVENTION OF CRIME AND THE TREATMENT OF OFFENDERS

## AT COMPUTER CRIME WORKSHOP

**April 15th, 2000**
**Vienna, Austria**

***As-delivered***

Thank you Mr. Chair. Good morning, everyone. It is a pleasure to be here.

Today's workshop will be looking at the relatively new problem of internet and computer crime.

A short ten years ago the internet was in its commercial infancy. Now, the proliferation of the internet and the technologies associated with it has, in a very real manner, revolutionized our world. It has changed the way we communicate with one another, the way we share information, the way we relate to each other.

Computer networks, and the internet, in particular, have managed to shrink our vast world. Today's technology allows us to share information with people in other countries, and on other continents with minimal expense.

With the internet the possibility now exists for people all over the world to have access to the stores of knowledge and products and services that were once only accessible by a very few. This possibility has provided new opportunities to draw the world together. The emergence of e-commerce is allowing small businesses around the world to compete with their larger competitors.

But, the internet has also created corresponding opportunities for criminals. Like everyone else, criminals have embraced high technology to further their goals.

We are becoming increasingly aware of the threats posed by the internet. Hate literature and child pornography can be disseminated easily. Even traditional crimes such as fraud and forgery can now be committed with the aid of the internet. Hackers can wreak havoc on our economic infrastructure by bringing down critical systems. Serious havoc can even result from a prank. There have been incidents where teenagers, either unknowingly or without understanding the full implications of their actions, have hacked into sensitive sites. That being said, the potential damage from a concerted attack by cyber-terrorists on a country's critical infrastructure could be catastrophic.

However, we cannot allow these threats to overshadow the immense benefits of the internet. Creative and innovative thinkers have dominated the computer age, and our solutions will also require creativity and innovative thinking. Our job, as lawmakers, law enforcement personnel, and industry representatives, is to work together to find solutions to deal with the threats posed by those who would abuse the internet, so as to preserve its benefits for the rest of society. We must take a multi-faceted approach.

First, we need laws that will criminalize computer-related crime. Second, we need to develop adequate procedural laws to enable us to investigate and prosecute cyber criminals. Third, we need government and industry to work together toward the common goal of controlling computer crime so as to make the internet as safe a place as possible. Finally, we need improved international cooperation in order to trace criminals on the internet.

Many countries have recognized the need to criminalize offences committed against or with the aid of computers. It is imperative, however, that all countries co-ordinate their efforts so that no country becomes a safe haven for criminals. If some countries criminalize certain conduct, and other countries do not, effective enforcement will be hindered.

Criminals will quickly learn which countries are the weak links in the enforcement chain and will take advantage of our inability to investigate, prosecute or extradite them. We must therefore work together to develop an international consensus as to what types of technology-related conduct should be criminalized and subject to extradition.

Our second task is to develop consensus with respect to procedural laws. This must all be accomplished in the new internet context, where many of our traditional law enforcement methods may not be applicable. The internet is everywhere and instant. These two very positive characteristics are also the source of almost all procedural impediments to internet related law enforcement.

We need to develop laws that will give law enforcement the ability to conduct computer crime investigations in a timely and efficient manner. The current measures in place for mutual legal assistance can hinder an investigation. These measures need to be improved.

The immediate nature of the internet and fragility of computer evidence requires that many crimes be investigated in "real time"; that is, investigated while the crime is occurring. We need laws that will enable us to trace communications throughout our own territories, but also into and throughout other countries with improved international cooperation.

Not only must law enforcement have the ability to trace communications while they are occurring, but they also must be able to trace the activity of criminals for past crimes. This requires, however, that traffic data - that is, data about the time and route of communications - be kept for a period of time by service providers. One impediment to effective tracing is that such traffic data is often not retained by service providers, or only retained for a short time.

In some cases, privacy laws require its quick deletion.

It is important that we come to some agreement, and with the participation of industry, as to the appropriate period of retention that will assist law enforcement in performing its duties to the public while still protecting the privacy of individual citizens. In order to retain the cooperation of industry, we need to keep their interests, such as compatibility of systems and financial and technical burdens, in mind when developing new laws.

In Canada, we have recently dealt with the issue of retention and use of personal information in the private sector. In a recent bill before Parliament concerning electronic commerce, we had to balance the privacy of personal data, its retention and deletion, and the needs of government and law enforcement to access that data in the fulfillment of their public duties.

In doing so, we consulted broadly with industry, law enforcement and other interest groups in order to achieve this balance. Search and seizure of electronic data pose a variety of domestic cyber crime problems. The intangible nature and transience of computer data, the complex and continuously evolving equipment, the possibility of networks existing in multiple jurisdictions, and the shortage of adequately trained law enforcement personnel combine to make the proper collection of evidence a perpetual challenge.

The ability to conduct transborder searches is another key component to a global solution. Unlike traditional crimes where evidence is generally in close proximity to the perpetrator or to the scene of the crime, the internet allows criminals to store evidence in computers great distances away. Complicating this matter is the fact that a criminal can delete all or most evidence of a crime in a matter of keystrokes.

The transborder tracing of communications and search of data implicate many of the ideals specific to our own countries; the protection of human rights, democratic freedoms, privacy, and probably most importantly, our own sovereignty.

With these factors in mind the G8 has been working toward finding solutions to transborder computer related crime issues. In December 1997, justice and interior ministers of the G8 adopted a statement of principles and an action plan to address high-tech crime.

Since then, they have created a network with points of contact to provide law enforcement with rapid assistance on a 24-hour basis. Our aim should be to expand this network to every country so as to enable law enforcement personnel to investigate high-tech crime wherever and whenever in the world it might occur.

In October 1999, the G8 ministers of justice and the interior adopted a set of principles on transborder access to stored computer data. The principles cover many issues relevant to computer evidence; including, the secure rapid preservation of data, and transborder access to data through expedited mutual assistance, and in some cases direct transborder access in cases of public internet sites or with consent of an authorized user.

The Council of Europe is currently negotiating a convention on cyber-crime, which will address many of the issues that I have mentioned, such as criminalization, procedural laws and international cooperation.

In March 2000, justice ministers of Member States of the Organization of American States adopted a set of recommendations to address computer related crime.

The Commonwealth is also planning to undertake initiatives to assist its members in addressing high-tech crime problems. Some work was done by the United Nations a few years ago, such as the UN Manual on the Prevention and Control of Computer-Related Crime, published in 1994 and which the Government of Canada sponsored financially.

However, we believe that it is now time for the UN again to become more active. In this regard I would like to thank the UN Asia and Far East Institute for the Prevention of Crime and the Treatment of Offenders for inviting me here to address you, and for showing leadership by organizing this workshop.

It is clear from what I have said that solutions will not only be legal, but technological as well. Government must foster an environment in which industry is encouraged to develop the tools we need to keep pace with high-tech crime. We must also ensure that internet service providers become partners rather than adversaries in the detection and investigation of high-tech crime. Next month in Paris, representatives from industry and law enforcement have been invited by the G8 governments to discuss issues relating to industry and law enforcement cooperation. This is a good beginning, but dialogue with industry must be expanded throughout the world.

We also need to develop highly trained experts. Continuous training is therefore necessary for any experts in this area. Along with highly skilled personnel, we require state-of-the-art equipment. Criminals adopt the latest technologies, and so must those of us who seek to apprehend them.

It is also clear, that on an individual level, our own personal privacy is most threatened by some of the new technologies and by some of the proposed solutions. A balance must be struck.

We must encourage the development of new technologies and enact laws that safeguard our privacy, while at the same time giving full consideration to other societal values which may be implicated. Often these values compete with each other.

For example, deletion of traffic data, which is not required to be retained for business purposes by a service provider, is a measure to protect the privacy of users. However, without the retention of such data for some period of time, the tracing of criminals who violate the integrity or confidentiality of computer systems can be rendered impossible.

The underlying reality is that any legislative measures we adopt, whether domestically or internationally, to address high-tech crime will have to involve a re-thinking of our basic notions of sovereignty, human rights and privacy. While it is imperative that we continue to protect all of those rights, we must also recognize that our current notions were formed in a context that is much different from the world in which we live today.

The landscape in which law enforcement now operates when investigating computer-related crime looks quite different from that of the past. Therefore, we have to adapt our laws and our thinking to accommodate this new reality. Without dispensing with our conceptions of human rights and sovereignty, we must find a way to adapt these notions to a new environment so that they apply to the world in which we live now.

In addition to creativity, our new challenges require courage. Courage to re-think our firmly held assumptions about how the world and our legal systems must operate, and courage to forge ahead with the bold steps necessary to confront the challenges facing us in this new age. With creativity and courage, we can overcome these challenges, make the internet safe and preserve our basic freedoms and values.

Thank you.

Date Modified: **2008-04-14**